

REMARKS

Reconsideration of the above identified application in view of the preceding amendments and following remarks is respectfully requested. Claims 1-32, 35 and 36 are pending in this application.

In the Office Action, Claims 1, 2, 5, 6, 7-9, 17, 18, 21-25 and 36 were rejected under 35 U.S.C. §103(a) over U.S. Patent No. 6,018,724 to Arent and further in view of U.S. Patent No. 5,708,655 to Toth et al.

Arent discloses a method for authenticating on-line transactions. The method is intended to address situations where a customer requests a proof of certification of a merchant. According to the Arent method, a certification authority must have pre-certified the merchant and provided the merchant with a digital certificate. In response to a customer's request for proof of certification, the Arent method contemplates that the merchant provides a digital certificate to the customer. The customer verifies the authenticity of the digital certificate with a software key which is publicly available. The software key may be unique to the customer. Upon verification, a certification indicator is visually displayed to the customer. For subsequent transactions, a merchant sends the same digital certificate to customer(s) and the customer(s) once again utilize the same software key for verification. Further, according to the Arent method, a plurality of merchants all utilize the same digital certificate and a plurality of customers repeatedly utilize the same, albeit unique, software keys for verification. The customer may customize their certification indicator with a text string. The digital certificate, the software keys, and certification indicator, whether customized or not, are reused repeatedly. Moreover, the text string which customizes the certification indicator is fixed, static and permanent. The text string is not used to perform the certification in order to establish a secure connection. Thus, if a merchant's digital

certificate is stolen, the digital certificate will continue to function to improperly indicate secure access.

Toth et al. disclose a method and apparatus for addressing a wireless communication station with a dynamically assigned address as applied in the field of cellular telephony. Upon termination of communication with the communication station, the dynamically assigned address can be reassigned and reused for communications with another station. The object of Toth et al. is to optimize the routing of data to roaming communication stations when the communication station does not have a permanent address with the host. For example, in cellular telephony, packets of data require an address. The address must be assigned to the destination communication station. However, communication stations may roam through networks. Toth et al. teach assigning a temporary address to each communication station in order to allow the station to receive packets of data. By assigning a temporary address to the station, the host can route packets directly to the station without having to access the home network of the station. Thus, the packets of data to the station are routed more efficiently. Problems associated with a limited supply of permanent addresses are avoided because the temporarily assigned address can be subsequently reassigned after deactivation of the station with the host (col. 7, lns. 22-27). Security is a problem because the packets of data travel across shared channels. Thus, when a secure communication is desired conventional authentication procedures are required (block 87 of Fig. 2, col. 8, lns. 46-54). In short, Toth et al. disclose an infrastructure for efficiently routing data to roaming communication stations. Toth et al. do not address authentication for security but for the limited section cited above which recognizes that conventional methods can be used to address the security issues.

It is respectfully submitted that one skilled in the art to which the subject invention appertains would not have been motivated to combine Arent with Toth et al. as

suggested by the Examiner. Arent shows the use of a reusable digital certificate with a reusable software key for on-line transactions. When the certificate or key is stolen, the thief is allowed improper access. Toth et al. adds nothing to the art in the related field of secure transactions let alone this particular problem but rather is directed solely to assigning temporary addresses to a roaming communication station in order to efficiently route packets of data. Toth et al.'s sole reference to authentication procedures is to describe them as conventional and required (see col. 8, lns. 46-53). Toth et al. does not serve the intended purpose of providing secure transactions in any way. Since Toth et al. is irrelevant neither reference can provide a motivation, teaching or suggestion to combine these references in the manner suggested by the Examiner. Accordingly, applicant's representative asserts that Claims 1, 2, 5, 6, 7-9, 17, 18, 21-25 and 36 are patentable over the combination of Arent and Toth et al.

Furthermore, even if combined, for the sake of argument, there is nothing in either Arent or Toth et al., either alone or in combination, in whole or in part, which discloses or suggests, a system as recited in Claims 1 and 17. If the two references were combined, one would have the infrastructure of Toth et al. for routing information with the authentication process of Arent. In contrast, Claims 1 and 17 recite a system and method including, *inter alia*, at least two parts or stations wherein a transaction or connection between any two or more of the parts or stations is conducted or established by means of an access code wherein the access code is selected from a plurality of codes at the time of conducting the transaction or establishing the connection such that no two transactions are conducted or no two connections are established with the same access code. Consequently, the access codes used for security are unique, stored at two locations and only used once. Because every transaction uses a new and different access code, the security and reliability of the transaction and environment is significantly increased. As a result, the user's code cannot be easily intercepted, stolen and improperly

used because the access code is never the same. A code stolen during authentication cannot be used for any purpose which solves the problem identified in Arent. Toth et al. in no way addresses this problem. Accordingly, Claims 1, 17 and each of the claims depending therefrom are not rendered obvious by the combination of references cited by the Examiner, and withdrawal of the rejection under 35 U.S.C. §103(a) is respectfully requested.

Furthermore, there is nothing in Arent or Toth et al. that discloses or suggests, either alone or in combination, in whole or in part, the device defined by Claim 36 of the subject application. In particular, none of the cited references disclose or suggest, either alone or in combination, in whole or in part, a method including the steps of providing a memory device for storing a first set of codes, wherein the memory device can receive, store and delete sets of codes which are accessible by the customer; storing a plurality of sets of codes with the provider, wherein the plurality of sets of codes includes the first set of codes; receiving a first customer code from the customer during establishing a secure connection, the first code being selected from the first set of codes stored on the memory device; accessing a first provider code from the first set of codes stored with the provider; comparing the first customer code with the first provider code, wherein a perfect match is a successful verification; establishing a secure connection to the customer when a successful verification occurs; and preventing further use of the first customer code by the customer by deleting the first customer code and the first provider code. Consequently, an access code can be used only once which prevents unauthorized subsequent use. As noted above, Arent has the shortcoming of repeatedly using a customized certification indicator without variation thereafter. Accordingly, for at least these reasons claim 36 is not rendered obvious by the combination of references and withdrawal of the rejection under 35 U.S.C. § 103(a) is respectfully requested.

In the Office Action, Claims 14, 16, 30, 32 and 35 were rejected under 35 U.S.C. §103(a) over U.S. Patent No. 6,018,724 to Arent in view of U.S. Patent No. 5,696,909 to Wallner and further in view of U.S. Patent No. 5,708,655 to Toth et al.

As noted above, Arent discloses a merchant-provided digital certificate methodology in which the certificate is verified with a customer software key. The digital certificate and the software key are not the same. According to the Arent methodology, neither the digital certificate nor the software key are modified, varied or altered during repeated use.

Also as noted above, Toth et al. discloses temporarily assigning an address to a communication station so that a host can directly route packets of data to such a communication station. Separate, conventional authentication is still required.

Wallner discloses a virtual terminal for processing transactions.

It is respectfully submitted that one skilled in the art to which the subject invention appertains would not have been motivated to combine Arent, Wallner and Toth et al. as suggested by the Examiner. Arent shows the use of a reusable digital certificate with a reusable software key for on-line transactions. When the certificate or key is stolen, the thief is allowed improper access. Toth et al. does not add anything to address the particular problem of access codes stolen during use being reusable but rather is directed solely to assigning a temporary address to a roaming communication station in order to efficiently route packets of data. Toth et al.'s sole reference to authentication procedures is to describe them as conventional and required (see col. 8, lns. 46-53). Toth et al. does not serve the intended purpose of providing secure transactions in any way. Since Toth et al. is irrelevant none of the references can provide a motivation, teaching or suggestion to combine the references in the manner suggested by the Examiner. Accordingly, applicant's representative asserts that Claims 14, 16, 30, 32 and 35 are patentable over the combination of Arent, Wallner and Toth et al.

Moreover, even if combined for the sake of argument, it is respectfully submitted that Wallner and Toth et al. do not overcome the deficiency of being able to inappropriately use a stolen digital certificate or software key noted with respect to Arent above. In particular, neither Arent, Wallner nor Toth et al. disclose or suggest, either alone or in combination, in whole or in part, a system including, *inter alia*, at least two stations wherein the access code is one of a plurality of codes provided to the accessed station and available to the accessing station, the access code being selected from the plurality of codes at the time of conducting the transaction such that no two transactions are conducted with the same access code as recited by Claims 1 and 17. Consequently, according to the presently claimed system, each access code is unique, stored at two locations and only used once. A code stolen during authentication cannot be used for any purpose which solves the problem identified in Arent. Accordingly, Claims 14, 16, 30 and 32 are not rendered obvious by the combination of references and withdrawal of the rejection under 35 U.S.C. §103(a) is respectfully requested.

Furthermore, there is nothing in Arent, Wallner or Toth et al. that discloses or suggests, either alone or in combination, in whole or in part, the device defined by Claim 35 of the subject application. In particular, none of the cited references disclose or suggest, either alone or in combination, in whole or in part, a method including, *inter alia*, the steps of providing a memory device for storing a first set of codes, wherein the memory device can receive, store and delete sets of codes which are accessible by the customer; storing a plurality of sets of codes with the provider, wherein the plurality of sets of codes includes the first set of codes; receiving a first customer code from the customer during establishing a secure connection, the first code being selected from the first set of codes stored on the memory device; accessing a first provider code from the first set of codes stored with the provider; comparing the first customer code with the first provider code, wherein a perfect match is a successful

verification; establishing a secure connection to the customer when a successful verification occurs; and preventing further use of the first customer code by the customer by deleting the first provider code. Consequently, two copies of the access codes exist, one at the customer and one at the provider until the first code is used and deleted. The customer does not generate the codes. However, the customer does transmit the codes to the provider to establish a secure connection. As noted above, Arent has the shortcoming of repeatedly using a customized certification indicator without variation thereafter. Neither Wallner nor Toth et al. overcome this deficiency. Accordingly, claim 35 is not rendered obvious by the combination of references and withdrawal of the rejection under 35 U.S.C. § 103(a) is respectfully requested.

In the Office Action, Claims 10 and 26 were rejected under 35 U.S.C. §103(a) over U.S. Patent No. 6,018,724 to Arent.

As noted above, Arent discloses a merchant-provided digital certificate which is verified with a customer software key. The digital certificate and the software key are not the same. Neither the digital certificate nor the software key are modified during repeated use. Thus, if a digital certificate is stolen, the theft of identity may be repeated over a period of time until the rightful owner discovers the theft and endeavors to cease the improper activity.

It is respectfully submitted that Arent does not disclose or suggest, in whole or in part, an invention including, *inter alia*, at least two stations wherein a transaction between any two stations is conducted by means of an access code, the access code being selected from the plurality of codes at the time of conducting the transaction such that no two transactions are conducted with the same access code as recited by Claims 1 and 17. Consequently, each access code is unique, stored at two locations and only used once. Accordingly, Claims 10 and 26, at least by virtue of their dependency upon Claims 1 and 17, respectively, are not rendered obvious by the reference cited by

the Examiner and withdrawal of the rejection under 35 U.S.C. §103(a) is respectfully requested.

In the Office Action, Claims 3, 4, 11-13, 15, 19, 20, 27-29 and 31 were rejected under 35 U.S.C. §103(a) over U.S. Patent No. 6,018,724 to Arent in view of U.S. Patent No. 4,630,201 to White and further in view of U.S. Patent No. 5,708,655 to Toth et al.

As noted above, Arent discloses a merchant-provided digital certificate which is verified with a customer software key. The digital certificate and the software key are not the same. Neither the digital certificate nor the software key are modified, varied or altered during repeated use.

White discloses an on-line transaction security system having a portable transaction device 34 and a central processor 20. The transaction device 34 receives a smart memory card to conduct a transaction. At the time of transaction, the transaction device 34 and the central processor 20 each generate a security code by algorithmically combining a transaction number (e.g., check number) and a random number. Upon generation of the security code, the transaction device 34 transmits its security code to the central processor 20 where it is compared with the security code generated by the central processor 20.

Also as noted above, Toth et al. discloses temporarily assigning an address to a communication station so that a host can directly route packets of data to such communication station. Separate, conventional authentication is still required. In contrast to the Examiner's characterization, it is respectfully submitted that Toth et al. does not teach, suggest or disclose employing different dynamically assigned access codes so that no two repeat.

It is respectfully submitted that Arent, White and Toth et al. is an improper combination as Toth et al. adds nothing to the art of authentication and therefore one

skilled in the art would not be motivated to combine such references. Since Toth et al. is irrelevant none of the references can provide a motivation, teaching or suggestion to combine the references in the manner suggested by the Examiner. Accordingly, applicant's representative asserts that Claims 3, 4, 11-13, 15, 19, 20, 27-29 and 31 are patentable over the combination of Arent, White and Toth et al.

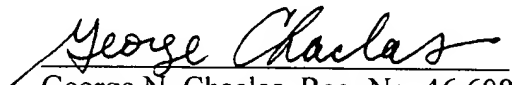
In any event, for the sake of argument, the cited combination of references does not disclose or suggest, either alone or in combination, in whole or in part, a system including, *inter alia*, a system and method including, *inter alia*, at least two parts or stations wherein a transaction or connection between any two or more of the parts or stations is conducted or established by means of an access code wherein the access code is selected from a plurality of codes at the time of conducting the transaction or establishing the connection such that no two transactions are conducted or no two connections are established with the same access code as recited by Claims 1 and 17. Consequently, each access code is unique, only used once and stored at the two parts prior to the time of transaction. The codes of the subject claim are used directly without algorithmic calculation. No skipping of codes or additional apparatus to generate the codes is required as in White. Thus, the use of codes directly is more efficient than that of the Arent and/or White methodology. Arent in no way helps to overcome this deficiency. Accordingly, Claims 1, 17 and each of the claims depending therefrom are not rendered obvious by the combination of references and withdrawal of the rejection under 35 U.S.C. §103(a) is respectfully requested.

Any additional fees or overpayments due as a result of filing the present paper may be applied to Deposit Account No. 50-1631. It is respectfully submitted that all of the claims now remaining in this application, namely Claims 1-32, 35 and 36, are in condition for allowance, and such action is earnestly solicited.

If after reviewing this Amendment, the Examiner believes that a telephone interview would facilitate the resolution of any remaining matters the undersigned attorney may be contacted at the number set forth hereinbelow.

Respectfully submitted,

Date : *July 15, 2002*


George N. Chaclas, Reg. No. 46,608
Cummings & Lockwood
Attorney for Applicant
CityPlace I
185 Asylum Street
Hartford, CT 06103
Tel: (860) 275-7045

.HrtLib1:400115.1 07/15/02